SANGFOR
深信服科技

SSL自动构建参数
单点登陆配置指导

深信服科技有限公司

2013 年 8 月

目录

第一章 单点登录简介

（1）什么是单点登录？

单点登录（Single Sign On），简称为 SSO，就是通过用户的一次性鉴别登录，即可获得需访问系统和应用软件的授权，用户无需多次输入用户名和密码，避免了密码外泄的风险。

（2）单点登录有哪些实现方式？

SSL VPN 的单点登录主要分为：

自动填表：用户在登录 SSL 控制台以后，需要借助单点登录助手在 WEB 页面或应用程序登录页面录制单点登录；自动填表的单点登录功能支持所有 WEB 应用，TCP 应用 ，L3VPN 和远程应用的所有 B/S 和 C/S 应用。

自动构建参数：用户在录制 SSL 单点登录的时候，不使用单点登录助手，而是手动填写相应单点登录各个参数信息；自动构建参数的单点登录方式只支持 WEB 应用，TCP 和 L3VPN 的 HTTP，HTTPS 应用。

第二章 单点登录配置流程

本文只介绍自动构建参数单点登录配置，自动填表方式单点登录配置参考:

http://sangfor.360help.com.cn/read.php?tid-5720.html

2.1 POST 请求方式配置

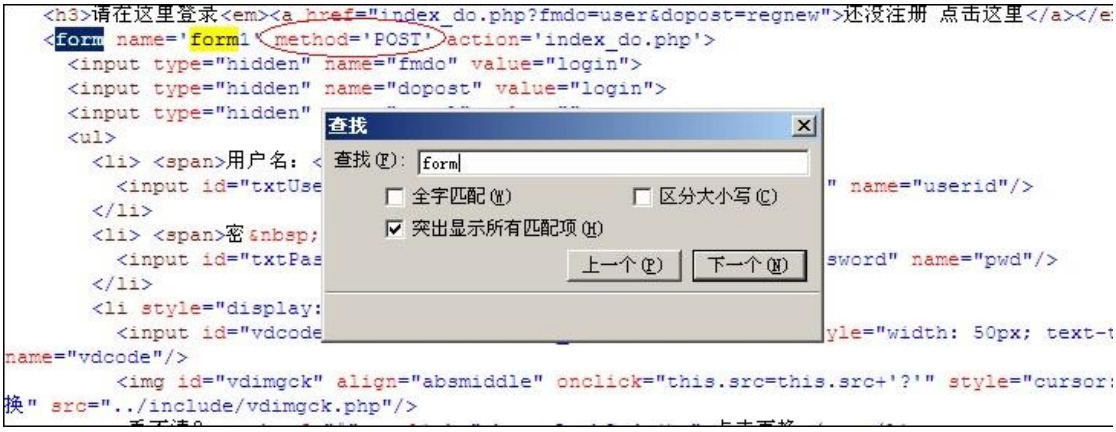
2.1.1 配置过程

配置思路为：启用单点登录→HTTPWATCH 抓取相关参数→配置相关参数。具体配过过程如下。

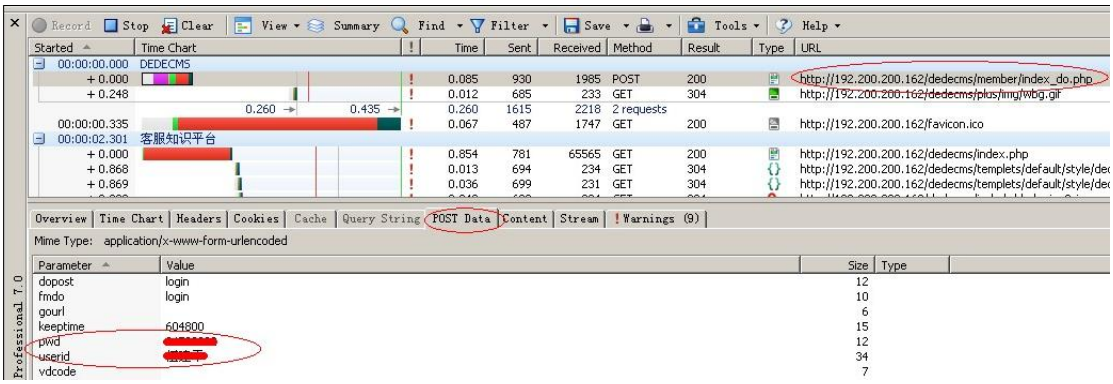
（1）登录控制台→系统设置→SSLVPN 选项→系统选项→单点登录，启用单点登录， 并勾上允许用户修改单点登录用户密码。

（2）用 IE 打开客户需要配置单点登录的资源，在网页上右键选择查看源文件。然后在源文件页面查找字段“charset”,下图就可以看出页面的编码方式为 UTF-8。

然后再查找字段“form”，下图可以看出请求方式为 POST。

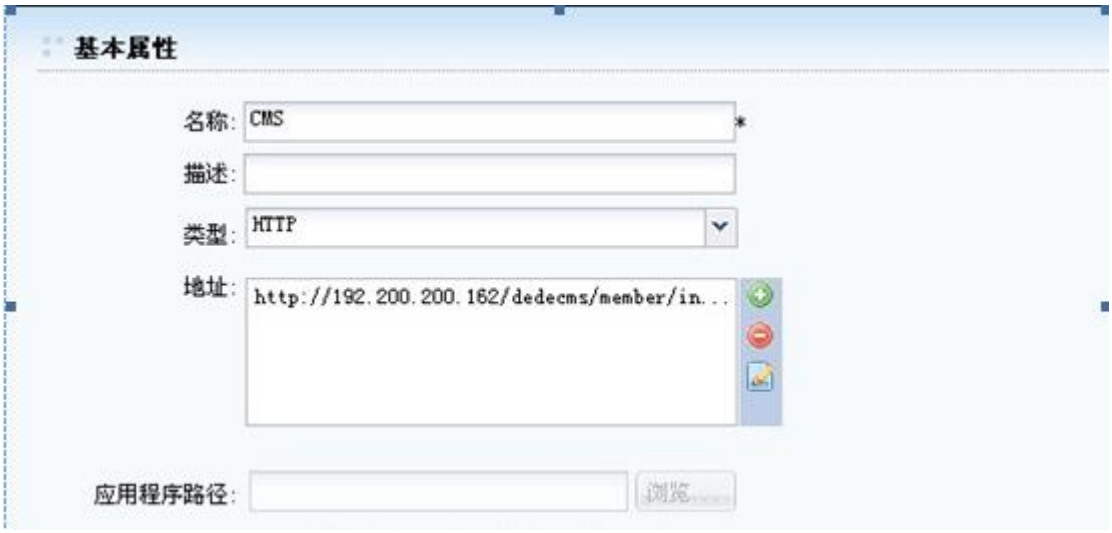


（3）打开 HTTPWATCH，在登陆页面输入用户名密码，然后登陆，查看 HTTPWATCH 抓出的参数，如下图：



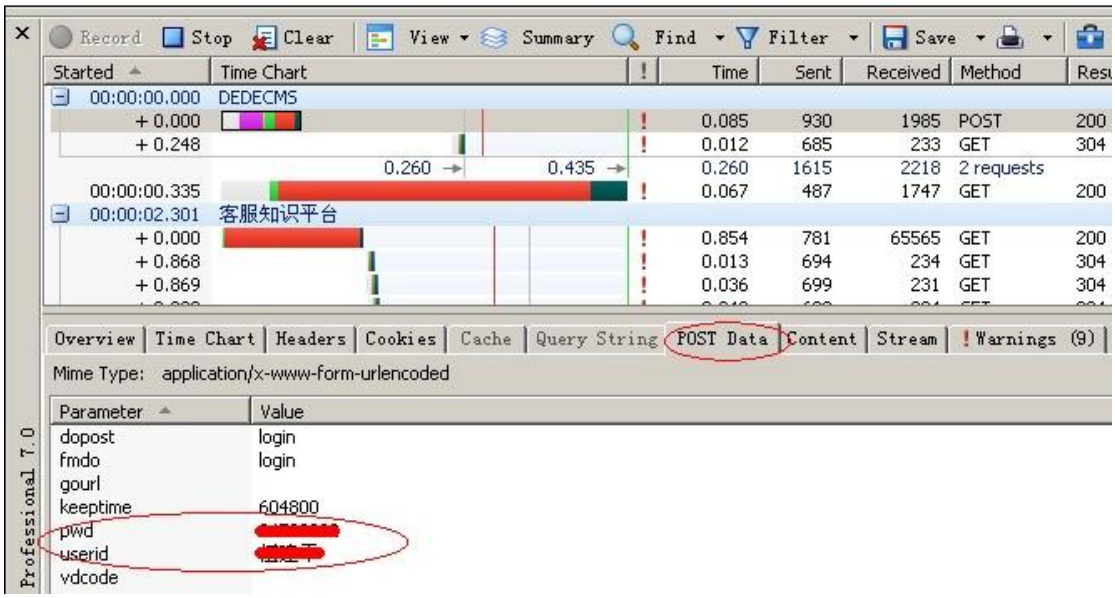
点击 POST 那一条，找到下面的 POST Data 这个项，我们可以得出几个参数就是，登陆页面的 URL：http://192.200.200.162/dedecms/member/index_do.php，还有用户名密码对应的参数，这里用户名对应的参数为：userid，密码对应的参数为：pwd 。

（4）新建资源，配置相关参数,地址里面填写前面抓到的登陆页面的 URL 填入。



启用单点登录，登陆方法：自动构建访问请求，请求方式：POST，编码：UTF-8,然后添加参数，参数名称 pwd,参数类型选择用户可配置密码和参数名称 userid,参数类型为用户可配置用户名，点击保存。然后测试。

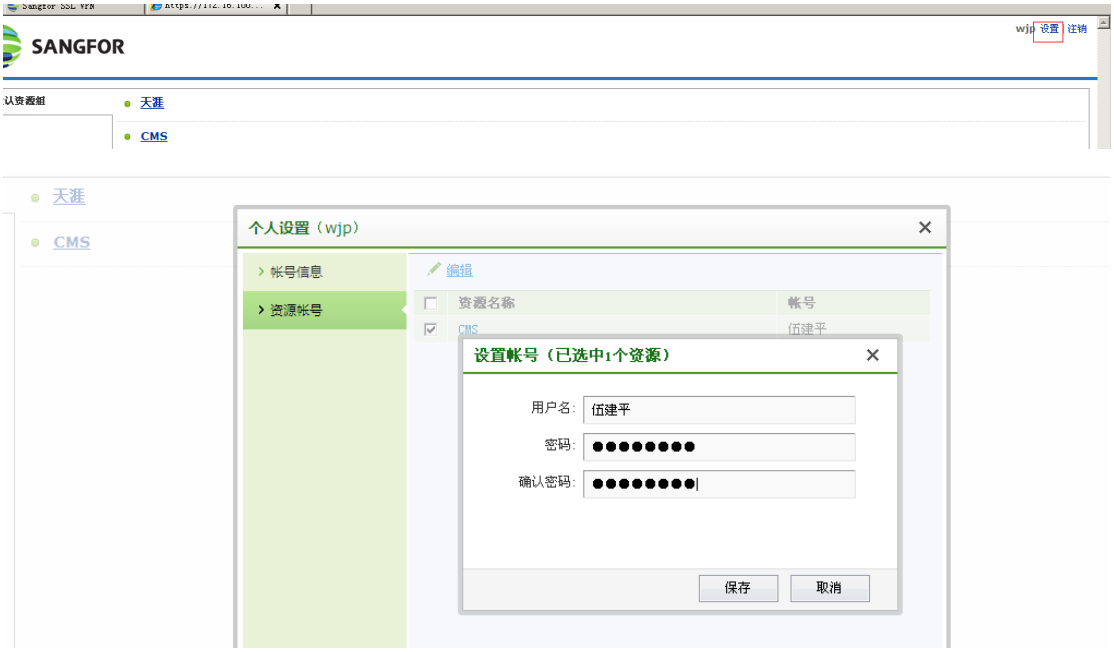
一般情况下填这 2 个参数就可以了，但是有的时候不会成功。因为有的页面除了提交用户名和密码 2 个参数之外，还需要提交其他参数，例如本案例，如果只添加用户名和密码两个参数，测试没有成功。不成功的话再回到 HTTPWATCH 抓包的页面：



发现除了用户名密码，还有其他参数，比如参数名为 keeptime 的值为 604600，把这几个参数都加进去。

2.1.2 效果展示

因为配置的时候选择的是用户可配置用户名和密码，所以第一次登陆的时候需要进个人设置里面设置登陆资源的账号和密码：

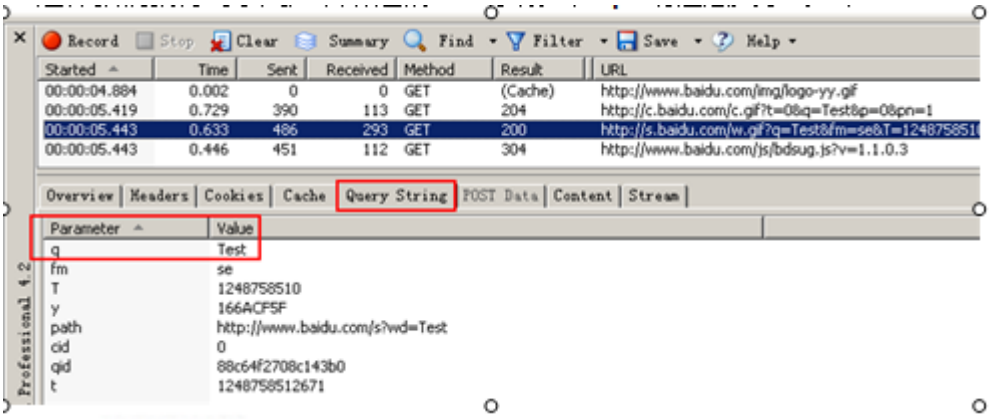


设置完之后点击保存，然后退出 VPN，重新登陆，点击资源，单点登录成功。

2.3 GET 请求方式配置

GET 请求的方式与 POST 请求方式的配置基本一致，只有 HTTPWATCH 抓包分析的地方有一点不同：

下图为 GET 方式的包，找到 GET 用户名密码的包，然后选择“Query String”选项卡，查看 GET 数据，找到需要的参数。



第三章 注意事项

1.只支持从资源页面点击链接的时候才会自动登陆，不支持在资源页面URL地址框直接输入地址或者重开IE 输入地址。

2.不支持带图形校验码的页面，因为图形信息无法预先获取，也不是固定值。

3.如果网页是除utf-8 和gb2312（gbk）以外的其他编码方式，是不支持的，需要定制。

4.不支持登录时会用到挑战码，或者调用脚本的登录方式。因为挑战中标准的是需要用户在用户密码认证成功后再次手动提交挑战信息，目前实现只能模拟表单提交。

5.只有同时满足以下几个条件的用户才能自己修改登陆资源的账号密码：（1）勾选了允许用户修改单点登录用户名密码。（2）该用户为私有用户。（3）配置参数时候选择的是用户可配置用户名或者用户可配置密码。

简而言之，websso 只对单纯的靠用户名,密码等固定值提交的网页才能适用，涉及到验证码等随机验证组件，以及其他需要用户配合的二次认证（即二次填写认证信息），等情况不可用。操作前必须知道认证方式可不可以简单的靠模拟表单提交就能认证通过，后台的认证方式是什么。